



Red Hat Virtualization 4.4

Upgrade Guide

Update and upgrade tasks for Red Hat Virtualization

Red Hat Virtualization 4.4 Upgrade Guide

Update and upgrade tasks for Red Hat Virtualization

Red Hat Virtualization Documentation Team

Red Hat Customer Content Services

rhev-docs@redhat.com

Legal Notice

Copyright © 2021 Red Hat, Inc.

The text of and illustrations in this document are licensed by Red Hat under a Creative Commons Attribution–Share Alike 3.0 Unported license ("CC-BY-SA"). An explanation of CC-BY-SA is available at

<http://creativecommons.org/licenses/by-sa/3.0/>

. In accordance with CC-BY-SA, if you distribute this document or an adaptation of it, you must provide the URL for the original version.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, the Red Hat logo, JBoss, OpenShift, Fedora, the Infinity logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux[®] is the registered trademark of Linus Torvalds in the United States and other countries.

Java[®] is a registered trademark of Oracle and/or its affiliates.

XFS[®] is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL[®] is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js[®] is an official trademark of Joyent. Red Hat is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack[®] Word Mark and OpenStack logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

A comprehensive guide to upgrading and updating components in a Red Hat Virtualization environment.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE	4
PART I. UPGRADING A STANDALONE MANAGER, LOCAL DATABASE ENVIRONMENT	5
CHAPTER 1. UPGRADING FROM 4.2 TO RED HAT VIRTUALIZATION 4.3	6
1.1. PREREQUISITES	6
1.2. ANALYZING THE ENVIRONMENT	6
1.3. UPDATING THE RED HAT VIRTUALIZATION MANAGER	7
1.4. UPGRADING THE MANAGER FROM 4.2 TO 4.3	8
1.5. UPDATING ALL HOSTS IN A CLUSTER	10
1.6. CHANGING THE CLUSTER COMPATIBILITY VERSION	11
1.7. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	12
1.8. CHANGING THE DATA CENTER COMPATIBILITY VERSION	12
1.9. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES	13
CHAPTER 2. UPGRADING FROM 4.3 TO RED HAT VIRTUALIZATION 4.4	16
2.1. PREREQUISITES	16
2.2. ANALYZING THE ENVIRONMENT	16
2.3. UPDATING THE RED HAT VIRTUALIZATION MANAGER	17
2.4. UPGRADING THE RED HAT VIRTUALIZATION MANAGER FROM 4.3 TO 4.4	18
2.5. MIGRATING HOSTS AND VIRTUAL MACHINES FROM RHV 4.3 TO 4.4	20
2.6. UPGRADING RHVH WHILE PRESERVING LOCAL STORAGE	21
2.7. CHANGING THE CLUSTER COMPATIBILITY VERSION	23
2.8. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	24
2.9. CHANGING THE DATA CENTER COMPATIBILITY VERSION	25
PART II. UPGRADING A STANDALONE MANAGER REMOTE DATABASE ENVIRONMENT	26
CHAPTER 3. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM 4.2 TO RED HAT VIRTUALIZATION 4.3	27
3.1. PREREQUISITES	27
3.2. ANALYZING THE ENVIRONMENT	27
3.3. UPGRADING REMOTE DATABASES FROM POSTGRESQL 9.5 TO 10	28
3.4. UPDATING THE RED HAT VIRTUALIZATION MANAGER	30
3.5. UPGRADING THE MANAGER FROM 4.2 TO 4.3	31
3.6. UPDATING ALL HOSTS IN A CLUSTER	32
3.7. CHANGING THE CLUSTER COMPATIBILITY VERSION	34
3.8. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	34
3.9. CHANGING THE DATA CENTER COMPATIBILITY VERSION	35
3.10. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES	35
CHAPTER 4. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM 4.3 TO RED HAT VIRTUALIZATION 4.4	39
4.1. PREREQUISITES	39
4.2. ANALYZING THE ENVIRONMENT	39
4.3. UPDATING THE RED HAT VIRTUALIZATION MANAGER	40
4.4. UPGRADING THE RED HAT VIRTUALIZATION MANAGER FROM 4.3 TO 4.4	41
4.5. UPGRADING REMOTE DATABASES FROM POSTGRESQL 10 TO 12	43
4.6. MIGRATING HOSTS AND VIRTUAL MACHINES FROM RHV 4.3 TO 4.4	44
4.7. UPGRADING RHVH WHILE PRESERVING LOCAL STORAGE	45
4.8. CHANGING THE CLUSTER COMPATIBILITY VERSION	48
4.9. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	48
4.10. CHANGING THE DATA CENTER COMPATIBILITY VERSION	49

PART III. UPGRADING A SELF-HOSTED ENGINE ENVIRONMENT	50
CHAPTER 5. UPGRADING A SELF-HOSTED ENGINE FROM 4.2 TO RED HAT VIRTUALIZATION 4.3	51
5.1. PREREQUISITES	51
5.2. ANALYZING THE ENVIRONMENT	51
5.3. ENABLING GLOBAL MAINTENANCE MODE	52
5.4. UPDATING THE RED HAT VIRTUALIZATION MANAGER	53
5.5. UPGRADING THE MANAGER FROM 4.2 TO 4.3	54
5.6. DISABLING GLOBAL MAINTENANCE MODE	55
5.7. UPDATING ALL HOSTS IN A CLUSTER	56
5.8. CHANGING THE CLUSTER COMPATIBILITY VERSION	57
5.9. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	58
5.10. CHANGING THE DATA CENTER COMPATIBILITY VERSION	58
5.11. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES	59
CHAPTER 6. UPGRADING A SELF-HOSTED ENGINE FROM 4.3 TO RED HAT VIRTUALIZATION 4.4	63
6.1. PREREQUISITES	63
6.2. ANALYZING THE ENVIRONMENT	63
6.3. MIGRATING VIRTUAL MACHINES FROM THE SELF-HOSTED ENGINE HOST	64
6.4. ENABLING GLOBAL MAINTENANCE MODE	64
6.5. UPDATING THE RED HAT VIRTUALIZATION MANAGER	65
6.6. UPGRADING THE RED HAT VIRTUALIZATION MANAGER FROM 4.3 TO 4.4	66
6.7. MIGRATING HOSTS AND VIRTUAL MACHINES FROM RHV 4.3 TO 4.4	68
6.8. UPGRADING RHVH WHILE PRESERVING LOCAL STORAGE	70
6.9. CHANGING THE CLUSTER COMPATIBILITY VERSION	72
6.10. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY	72
6.11. CHANGING THE DATA CENTER COMPATIBILITY VERSION	73
PART IV. APPENDICES	74
APPENDIX A. UPDATES BETWEEN MINOR RELEASES	75
A.1. ANALYZING THE ENVIRONMENT	75
A.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER	76
A.3. UPDATING A SELF-HOSTED ENGINE	77
A.4. UPDATING ALL HOSTS IN A CLUSTER	80
A.5. UPDATING INDIVIDUAL HOSTS	81
A.6. MANUALLY UPDATING HOSTS	83
APPENDIX B. UPDATING THE LOCAL REPOSITORY FOR AN OFFLINE RED HAT VIRTUALIZATION MANAGER INSTALLATION	86
B.1. ADDITIONAL RESOURCES	86

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code, documentation, and web properties. Because of the enormity of this endeavor, these changes are being updated gradually and where possible. For more details, see [our CTO Chris Wright's message](#).

PART I. UPGRADING A STANDALONE MANAGER, LOCAL DATABASE ENVIRONMENT

CHAPTER 1. UPGRADING FROM 4.2 TO RED HAT VIRTUALIZATION 4.3

Upgrading your environment from 4.2 to 4.3 involves the following steps:

1. [Make sure you meet the prerequisites, including enabling the correct repositories](#)
2. [Use the Log Collection Analysis tool to check for issues that might prevent a successful upgrade](#)
3. [Update the 4.2 Manager to the latest version of 4.2](#)
4. [Upgrade the Manager from 4.2 to 4.3](#)
5. [Update the hosts](#)
6. [Update the compatibility version of the clusters](#)
7. [Reboot any running or suspended virtual machines to update their configuration](#)
8. [Update the compatibility version of the data centers](#)
9. If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, [you must replace the certificates now](#).

1.1. PREREQUISITES

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.4. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).

1.2. ANALYZING THE ENVIRONMENT

Run the Log Collection Analysis tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them.

The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

1.3. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt*setup* rh*vm-setup-plugins
```

- Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

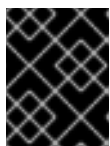


IMPORTANT

The update process might take some time. Do not stop the process before it completes.

- Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).

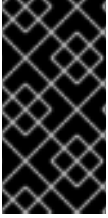


IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

1.4. UPGRADING THE MANAGER FROM 4.2 TO 4.3

Upgrade the Red Hat Virtualization Manager from 4.2 to 4.3.



IMPORTANT

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.
2. Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt*setup* rh*vm-setup-plugins
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

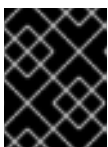
```
Execution of setup completed successfully
```

5. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.2-manager-rpms \
  --disable=jb-eap-7-for-rhel-7-server-rpms
```

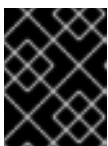
6. Update the base operating system:

```
# yum update
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

You can now update the hosts.

1.5. UPDATING ALL HOSTS IN A CLUSTER

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See https://github.com/oVirt/ovirt-ansible-collection/blob/master/roles/cluster_upgrade/README.md for more information about the Ansible role used to automate the updates.

Update one cluster at a time.

Limitations


- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If the cluster has migration enabled, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster. The **Upgrade status** column shows if an upgrade is available for any hosts in the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
 - **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.

- **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to **cluster_maintenance** during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.
5. Click **Next**.
 6. Review the summary of the hosts and virtual machines that will be affected.
 7. Click **Upgrade**.

You can track the progress of host updates:

- in the **Compute** → **Clusters** view, the **Upgrade Status** column shows **Upgrade in progress**
- in the **Compute** → **Hosts** view
- in the **Events** section of the **Notification Drawer** ().

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute** → **Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

1.6. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.



IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure


1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

1.7. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.

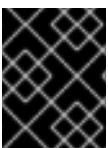


NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

1.8. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, you must do so now.

1.9. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES

Red Hat Virtualization 4.4 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures.

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. On the Manager, save a backup of the `/etc/ovirt-engine/engine.conf.d` and `/etc/pki/ovirt-engine` directories, and re-sign the certificates:

```
# ./etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
# for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
```

```
--subject="${subject}" \
--san=DNS:${ENGINE_FQDN}" \
--keep-key
done
```

- Restart the **httpd** service:

```
# systemctl restart httpd
```

- Connect to the Administration Portal to confirm that the warning no longer appears.
- If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

- Log in to the Manager machine as the root user.
- Check whether **/etc/pki/ovirt-engine/openssl.conf** includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

- Re-sign the CA certificate by backing it up and creating a new certificate in **ca.pem.new**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S")"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

- Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

- Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.

6. On the Manager, save a backup of the `/etc/ovirt-engine/engine.conf.d` and `/etc/pki/ovirt-engine` directories, and re-sign the certificates:

```
# ./etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
# for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --san=DNS:"${ENGINE_FQDN}" \
    --keep-key
done
```

7. Restart the following services:

```
# systemctl restart httpd
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-imageio
```

8. Connect to the Administration Portal to confirm that the warning no longer appears.
9. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **`http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA`**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).
10. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute** → **Hosts**.
 - b. Select the host and click **Management** → **Maintenance** and **OK**.
 - c. Once the host is in maintenance mode, click **Installation** → **Enroll Certificate**.
 - d. Click **Management** → **Activate**.

CHAPTER 2. UPGRADING FROM 4.3 TO RED HAT VIRTUALIZATION 4.4

Upgrading your environment from 4.3 to 4.4 involves the following steps:

1. [Make sure you meet the prerequisites, including enabling the correct repositories](#) .
2. [Use the Log Collection Analysis tool to check for issues that might prevent a successful upgrade.](#)
3. [Update the 4.3 Manager to the latest version of 4.3](#)
4. [Upgrade the Manager from 4.3 to 4.4](#) .
5. [Migrate hosts and virtual machines while reducing virtual machine downtime](#) .
6. [\(Optional\) Upgrade RHVH while preserving local storage](#) .
7. [Update the compatibility version of the clusters.](#)
8. [Reboot any running or suspended virtual machines to update their configuration](#) .
9. [Update the compatibility version of the data centers.](#)

2.1. PREREQUISITES

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.4. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#) .

2.2. ANALYZING THE ENVIRONMENT

Run the Log Collection Analysis tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them.

The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.3. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

You can now update the Manager to the latest version of 4.3.

2.3. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.3. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

■

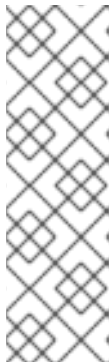
```
# yum update ovirt-*setup* rh-*vm-setup-plugins
```

- Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

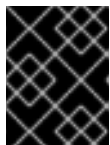


IMPORTANT

The update process might take some time. Do not stop the process before it completes.

- Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

You can now upgrade the Manager to 4.4.

2.4. UPGRADING THE RED HAT VIRTUALIZATION MANAGER FROM 4.3 TO 4.4

Red Hat Virtualization Manager 4.4 is only supported on Red Hat Enterprise Linux 8.2 or later. You need to do a clean installation of Red Hat Enterprise Linux 8.2 and Red Hat Virtualization Manager 4.4, even if you are using the same physical machine that you use to run RHV Manager 4.3.

The upgrade process requires restoring Red Hat Virtualization Manager 4.3 backup files onto the Red Hat Virtualization Manager 4.4 machine.

Prerequisites

- All data centers and clusters in the environment must have the cluster compatibility level set to version 4.2 or 4.3 before you start the procedure.
- If you use an external CA to sign HTTPS certificates, follow the steps in [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*. The backup and restore include the 3rd-party certificate, so you should be able to log in to the Administration portal after the upgrade. Ensure the CA certificate is added to system-wide trust stores of all clients to ensure the foreign menu of virt-viewer works. See [BZ#1313379](#) for more information.



NOTE

Connected hosts and virtual machines can continue to work while the Manager is being upgraded.

Procedure

1. Log in to the Manager machine.
2. Back up the Red Hat Virtualization Manager 4.3 environment.


```
# engine-backup --scope=all --mode=backup --file=backup.bck --log=backuplog.log
```
3. Copy the backup file to a storage device outside of the RHV environment.
4. Install Red Hat Enterprise Linux 8.2 or later. See [Performing a standard RHEL installation](#) for more information.
5. Complete the steps to install Red Hat Virtualization Manager 4.4, including running the command **yum install rhvm**, but do not run **engine-setup**. See one of the *Installing Red Hat Virtualization* guides for more information.
6. Copy the backup file to the Red Hat Virtualization Manager 4.4 machine and restore it.

```
# engine-backup --mode=restore --file=backup.bck --provision-all-databases
```



NOTE

If the backup contained grants for extra database users, this command creates the extra users with random passwords. You must change these passwords manually if the extra users require access to the restored system. See <https://access.redhat.com/articles/2686731>.

7. Install optional extension packages if they were installed on the Red Hat Virtualization Manager 4.3 machine.

```
# yum install ovirt-engine-extension-aaa-ldap ovirt-engine-extension-aaa-misc ovirt-engine-extension-logger-log4j
```

**NOTE**

The configuration for these package extensions must be manually reapplied because they are not migrated as part of the backup and restore process.

- Decommission the Red Hat Virtualization Manager 4.3 machine if a different machine is used for Red Hat Virtualization Manager 4.4. Two different Managers must not manage the same hosts or storage.
- Run **engine-setup** to configure the Manager.

```
# engine-setup
```

The Red Hat Virtualization Manager 4.4 is now installed, with the cluster compatibility version set to 4.2 or 4.3, whichever was the preexisting cluster compatibility version. Now you need to upgrade the hosts in your environment to RHV 4.4, after which you can change the cluster compatibility version to 4.4.

Additional resources

- [Installing Red Hat Virtualization as a standalone Manager with local databases](#)
- [Installing Red Hat Virtualization as a standalone Manager with remote databases](#)

You can now update the hosts.

2.5. MIGRATING HOSTS AND VIRTUAL MACHINES FROM RHV 4.3 TO 4.4

You can migrate hosts and virtual machines from Red Hat Virtualization 4.3 to 4.4 such that you minimize the downtime of virtual machines in your environment.

This process requires migrating all virtual machines from one host so as to make that host available to upgrade to RHV 4.4. After the upgrade, you can reattach the host to the Manager.

**WARNING**

When installing or reinstalling the host's operating system, Red Hat strongly recommends that you first detach any existing non-OS storage that is attached to the host to avoid accidental initialization of these disks, and with that, potential data loss.

Prerequisites

- Hosts for RHV 4.4 require Red Hat Enterprise Linux 8.2 or later. A clean installation of Red Hat Enterprise Linux 8.2 or later, or Red Hat Virtualization Host 4.4 is required, even if you are using the same physical machine that you use to run hosts for RHV 4.3.
- Red Hat Virtualization Manager 4.4 is installed and running.

- The compatibility level of the data center and cluster to which the hosts belong is set to 4.2 or 4.3. All data centers and clusters in the environment must have the cluster compatibility level set to version 4.2 or 4.3 before you start the procedure.

Procedure

1. Pick a host to upgrade and migrate that host's virtual machines to another host in the same cluster. You can use Live Migration to minimize virtual machine downtime. For more information, see [Migrating Virtual Machines Between Hosts](#) in the *Virtual Machine Management Guide*.
2. Put the host into maintenance mode and remove the host from the Manager. For more information, see [Removing a Host](#) in the *Administration Guide*.
3. Install Red Hat Enterprise Linux 8.2 or later, or RHVH 4.4. For more information, see [Installing Hosts for Red Hat Virtualization](#) in one of the *Installing Red Hat Virtualization* guides.
4. Install the appropriate packages to enable the host for RHV 4.4. For more information, see [Installing Hosts for Red Hat Virtualization](#) in one of the *Installing Red Hat Virtualization* guides.
5. Add this host to the Manager, assigning it to the same cluster. You can now migrate virtual machines onto this host. For more information, see [Adding Standard Hosts to the Manager](#) in one of the *Installing Red Hat Virtualization* guides.

Repeat these steps to migrate virtual machines and upgrade hosts for the rest of the hosts in the same cluster, one by one, until all are running Red Hat Virtualization 4.4.

Additional resources

- [Installing Red Hat Virtualization as a self-hosted engine using the Cockpit web interface](#)
- [Installing Red Hat Virtualization as a self-hosted engine using the command line](#)
- [Installing Red Hat Virtualization as a standalone Manager with local databases](#)
- [Installing Red Hat Virtualization as a standalone Manager with remote databases](#)

2.6. UPGRADING RHVH WHILE PRESERVING LOCAL STORAGE

Environments with local storage cannot migrate virtual machines to a host in another cluster because the local storage is not shared with other storage domains. To upgrade RHVH 4.3 hosts that have a local storage domain, reinstall the host while preserving the local storage, create a new local storage domain in the 4.4 environment, and import the previous local storage into the new domain.

Prerequisites

- Red Hat Virtualization Manager 4.4 is installed and running.
- The compatibility level of the data center and cluster to which the host belongs is set to 4.2 or 4.3.

Procedure

1. Ensure that the local storage on the RHVH 4.3 host's local storage is in maintenance mode before starting this process. Complete these steps:

- a. Open the **Data Centers** tab.
 - b. Click the **Storage** tab in the **Details** pane and select the storage domain in the results list.
 - c. Click **Maintenance**.
2. Reinstall the Red Hat Virtualization Host, as described in [Installing Red Hat Virtualization Host](#) in the *Installation Guide*.



IMPORTANT

When selecting the device on which to install RHVH from the **Installation Destination** screen, do not select the device(s) storing the virtual machines. Only select the device where the operating system should be installed.

If you are using Kickstart to install the host, ensure that you preserve the devices containing the virtual machines by adding the following to the Kickstart file, replacing ``device`` with the relevant device.

```
# clearpart --all --drives=device
```

For more information on using Kickstart, see [Kickstart references](#) in *Red Hat Enterprise Linux 8 Performing an advanced RHEL installation*.

3. On the reinstalled host, create a directory, for example **/data** in which to recover the previous environment.

```
# mkdir /data
```

4. Mount the previous local storage in the new directory. In our example, **/dev/sdX1** is the local storage:

```
# mount /dev/sdX1 /data
```

5. Set the following permissions for the new directory.

```
# chown -R 36:36 /data
# chmod -R 0755 /data
```

6. Red Hat recommends that you also automatically mount the local storage via **/etc/fstab** in case the server requires a reboot:

```
# blkid | grep -i sdX1
/dev/sdX1: UUID="a81a6879-3764-48d0-8b21-2898c318ef7c" TYPE="ext4"
# vi /etc/fstab
UUID="a81a6879-3764-48d0-8b21-2898c318ef7c" /data ext4 defaults 0 0
```

7. In the Administration Portal, create a data center and select **Local** in the **Storage Type** drop-down menu.
8. Configure a cluster on the new data center. See [Creating a New Cluster](#) in the *Administration Guide* for more information.

9. Add the host to the Manager. See [Adding Standard Hosts to the Red Hat Virtualization Manager](#) in one of the *Installing Red Hat Virtualization* guides for more information.
10. On the host, create a new directory that will be used to create the initial local storage domain. For example:


```
# mkdir -p /localfs
# chown 36:36 /localfs
# chmod -R 0755 /localfs
```
11. In the Administration Portal, open the **Storage** tab and click **New Domain** to create a new local storage domain.
12. Set the name to **localfs** and set the path to **/localfs**.
13. Once the local storage is active, click **Import Domain** and set the domain's details. For example, define **Data** as the name, **Local on Host** as the storage type and **/data** as the path.
14. Click **OK** to confirm the message that appears informing you that storage domains are already attached to the data center.
15. Activate the new storage domain:
 - a. Open the **Data Centers** tab.
 - b. Click the **Storage** tab in the details pane and select the new data storage domain in the results list.
 - c. Click **Activate**.
16. Once the new storage domain is active, import the virtual machines and their disks:
 - a. In the **Storage** tab, select **data**.
 - b. Select the **VM Import** tab in the details pane, select the virtual machines and click **Import**. See [Importing Virtual Machines from a Data Domain](#) in the *Virtual Machine Management Guide* for more details.
17. Once you have ensured that all virtual machines have been successfully imported and are functioning properly, you can move **localfs** to maintenance mode.
18. Click the **Storage** tab and select **localfs** from the results list.
 - a. Click the **Data Center** tab in the details pane.
 - b. Click Maintenance, then click **OK** to move the storage domain to maintenance mode.
 - c. Click **Detach**. The Detach Storage confirmation window opens.
 - d. Click **OK**.

You have now upgraded the host to version 4.4, created a new local storage domain, and imported the 4.3 storage domain and its virtual machines.

You can now update the cluster compatibility version.

2.7. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.



IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.




IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

You can now update the cluster compatibility version for virtual machines in the cluster.

2.8. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

You can now update the data center compatibility version.

2.9. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute → Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

PART II. UPGRADING A STANDALONE MANAGER REMOTE DATABASE ENVIRONMENT

CHAPTER 3. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM 4.2 TO RED HAT VIRTUALIZATION 4.3

Upgrading your environment from 4.2 to 4.3 involves the following steps:

1. [Make sure you meet the prerequisites, including enabling the correct repositories](#)
2. [Use the Log Collection Analysis tool to check for issues that might prevent a successful upgrade](#)
3. [Upgrade the database from PostgreSQL 9.5 to 10.0](#)
4. [Update the 4.2 Manager to the latest version of 4.2](#)
5. [Upgrade the Manager from 4.2 to 4.3](#)
6. [Update the hosts](#)
7. [Update the compatibility version of the clusters](#)
8. [Reboot any running or suspended virtual machines to update their configuration](#)
9. [Update the compatibility version of the data centers](#)
10. If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, [you must replace the certificates now](#).

3.1. PREREQUISITES

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.4. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).

3.2. ANALYZING THE ENVIRONMENT

Run the Log Collection Analysis tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them.

The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

3.3. UPGRADING REMOTE DATABASES FROM POSTGRESQL 9.5 TO 10

Red Hat Virtualization 4.3 uses PostgreSQL 10 instead of PostgreSQL 9.5. If your databases are installed locally, the upgrade script automatically upgrades them from version 9.5 to 10. However, if either of your databases (Manager or Data Warehouse) is installed on a separate machine, you must perform the following procedure on each remote database before upgrading the Manager.

1. Stop the service running on the machine:

- Stop the **ovirt-engine** service on the Manager machine:

```
# systemctl stop ovirt-engine
```

- Stop the **ovirt-engine-dwh** service on the Data Warehouse machine:


```
# systemctl stop ovirt-engine-dwhd
```

2. Enable the required repository to receive the PostgreSQL 10 package:
Enable either the Red Hat Virtualization Manager repository:

```
# subscription-manager repos --enable=rhel-7-server-rhv-4.3-manager-rpms
```

or the SCL repository:

```
# subscription-manager repos --enable rhel-server-rhscl-7-rpms
```

3. Install the PostgreSQL 10 packages:

```
# yum install rh-postgresql10 rh-postgresql10-postgresql-contrib
```

4. Stop and disable the PostgreSQL 9.5 service:

```
# systemctl stop rh-postgresql95-postgresql
# systemctl disable rh-postgresql95-postgresql
```

5. Upgrade the PostgreSQL 9.5 database to PostgreSQL 10:

```
# scl enable rh-postgresql10 -- postgresql-setup --upgrade-from=rh-postgresql95-postgresql
--upgrade
```

6. Start and enable the **rh-postgresql10-postgresql.service** and check that it is running:

```
# systemctl start rh-postgresql10-postgresql.service
# systemctl enable rh-postgresql10-postgresql.service
# systemctl status rh-postgresql10-postgresql.service
```

Ensure that you see output similar to the following:

```
rh-postgresql10-postgresql.service - PostgreSQL database server
Loaded: loaded (/usr/lib/systemd/system/rh-postgresql10-postgresql.service;
enabled; vendor preset: disabled)
Active: active (running) since ...
```

7. Copy the **pg_hba.conf** client configuration file from the PostgreSQL 9.5 environment to the PostgreSQL 10 environment:

```
# cp -p /var/opt/rh/rh-postgresql95/lib/pgsql/data/pg_hba.conf /var/opt/rh/rh-
postgresql10/lib/pgsql/data/pg_hba.conf
```

8. Update the following parameters in **/var/opt/rh/rh-postgresql10/lib/pgsql/data/postgresql.conf**:

```
listen_addresses='*'
autovacuum_vacuum_scale_factor=0.01
autovacuum_analyze_scale_factor=0.075
autovacuum_max_workers=6
```

```
maintenance_work_mem=65536
max_connections=150
work_mem = 8192
```

- Restart the PostgreSQL 10 service to apply the configuration changes:

```
# systemctl restart rh-postgresql10-postgresql.service
```

- Start the **ovirt-engine-dwhd** service:

```
# systemctl start ovirt-engine-dwhd
```

You can now update the Manager to the latest version of 4.2.

3.4. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

- On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

- Update the setup packages:

```
# yum update ovirt\*setup\* rh\*vm-setup-plugins
```

- Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

**NOTE**

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

**IMPORTANT**

The update process might take some time. Do not stop the process before it completes.

4. Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```

**IMPORTANT**

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the update.

You can now upgrade the Manager to 4.3.

3.5. UPGRADING THE MANAGER FROM 4.2 TO 4.3

Upgrade the Red Hat Virtualization Manager from 4.2 to 4.3.

**IMPORTANT**

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager machine.
2. Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt\*setup\* rh\*vm-setup-plugins
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

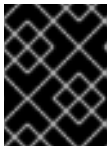
```
Execution of setup completed successfully
```

5. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
  --disable=rhel-7-server-rhv-4.2-manager-rpms \
  --disable=jb-eap-7-for-rhel-7-server-rpms
```

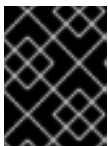
6. Update the base operating system:

```
# yum update
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

You can now update the hosts.

3.6. UPDATING ALL HOSTS IN A CLUSTER

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See https://github.com/oVirt/ovirt-ansible-collection/blob/master/roles/cluster_upgrade/README.md for more information about the Ansible role used to automate the updates.

Update one cluster at a time.

Limitations


- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.

- If the cluster has migration enabled, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster. The **Upgrade status** column shows if an upgrade is available for any hosts in the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
 - **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.
 - **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to **cluster_maintenance** during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.
5. Click **Next**.
6. Review the summary of the hosts and virtual machines that will be affected.
7. Click **Upgrade**.

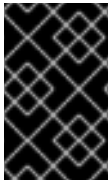
You can track the progress of host updates:

- in the **Compute** → **Clusters** view, the **Upgrade Status** column shows **Upgrade in progress**
- in the **Compute** → **Hosts** view
- in the **Events** section of the **Notification Drawer** ()

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute** → **Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

3.7. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.



IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure


1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

3.8. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ()

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that

has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

3.9. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, you must do so now.

3.10. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES

Red Hat Virtualization 4.4 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures.

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S)"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. On the Manager, save a backup of the `/etc/ovirt-engine/engine.conf.d` and `/etc/pki/ovirt-engine` directories, and re-sign the certificates:

```
# ./etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
# for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\); \1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --san=DNS:"${ENGINE_FQDN}" \
    --keep-key
done
```

5. Restart the **httpd** service:

```
# systemctl restart httpd
```

6. Connect to the Administration Portal to confirm that the warning no longer appears.
7. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **`http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA`**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Re-sign the CA certificate by backing it up and creating a new certificate in **ca.pem.new**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S")"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

4. Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```

5. Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.

6. On the Manager, save a backup of the `/etc/ovirt-engine/engine.conf.d` and `/etc/pki/ovirt-engine` directories, and re-sign the certificates:

```
# ./etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
# for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
```

```
--password=mypass \  
--subject="{subject}" \  
--san=DNS: "{ENGINE_FQDN}" \  
--keep-key  
done
```

7. Restart the following services:

```
# systemctl restart httpd  
# systemctl restart ovirt-engine  
# systemctl restart ovirt-websocket-proxy  
# systemctl restart ovirt-imageio
```

8. Connect to the Administration Portal to confirm that the warning no longer appears.
9. If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).
10. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute → Hosts**.
 - b. Select the host and click **Management → Maintenance** and **OK**.
 - c. Once the host is in maintenance mode, click **Installation → Enroll Certificate**.
 - d. Click **Management → Activate**.

CHAPTER 4. UPGRADING A REMOTE DATABASE ENVIRONMENT FROM 4.3 TO RED HAT VIRTUALIZATION 4.4

Upgrading your environment from 4.3 to 4.4 involves the following steps:

1. [Make sure you meet the prerequisites, including enabling the correct repositories](#)
2. [Use the Log Collection Analysis tool to check for issues that might prevent a successful upgrade](#)
3. [Update the 4.3 Manager to the latest version of 4.3](#)
4. [Upgrade the Manager from 4.3 to 4.4](#)
5. [Upgrade the database from PostgreSQL 10.0 to 12.0](#)
6. [Migrate hosts and virtual machines while reducing virtual machine downtime](#) .
7. [\(Optional\) Upgrade RHVH while preserving local storage](#) .
8. [Update the compatibility version of the clusters.](#)
9. [Reboot any running or suspended virtual machines to update their configuration](#) .
10. [Update the compatibility version of the data centers.](#)

4.1. PREREQUISITES

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.4. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#) .

4.2. ANALYZING THE ENVIRONMENT

Run the Log Collection Analysis tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them.

The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.3. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

-

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

You can now update the Manager to the latest version of 4.3.

4.3. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.3. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt*setup\* rh*vm-setup-plugins
```

3. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.



IMPORTANT

The update process might take some time. Do not stop the process before it completes.

4. Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the update.

You can now upgrade the Manager to 4.4.

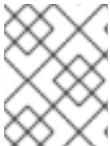
4.4. UPGRADING THE RED HAT VIRTUALIZATION MANAGER FROM 4.3 TO 4.4

Red Hat Virtualization Manager 4.4 is only supported on Red Hat Enterprise Linux 8.2 or later. You need to do a clean installation of Red Hat Enterprise Linux 8.2 and Red Hat Virtualization Manager 4.4, even if you are using the same physical machine that you use to run RHV Manager 4.3.

The upgrade process requires restoring Red Hat Virtualization Manager 4.3 backup files onto the Red Hat Virtualization Manager 4.4 machine.

Prerequisites

- All data centers and clusters in the environment must have the cluster compatibility level set to version 4.2 or 4.3 before you start the procedure.
- If you use an external CA to sign HTTPS certificates, follow the steps in [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*. The backup and restore include the 3rd-party certificate, so you should be able to log in to the Administration portal after the upgrade. Ensure the CA certificate is added to system-wide trust stores of all clients to ensure the foreign menu of virt-viewer works. See [BZ#1313379](#) for more information.



NOTE

Connected hosts and virtual machines can continue to work while the Manager is being upgraded.

Procedure

1. Log in to the Manager machine.
2. Back up the Red Hat Virtualization Manager 4.3 environment.

```
# engine-backup --scope=all --mode=backup --file=backup.bck --log=backuplog.log
```
3. Copy the backup file to a storage device outside of the RHV environment.
4. Install Red Hat Enterprise Linux 8.2 or later. See [Performing a standard RHEL installation](#) for more information.
5. Complete the steps to install Red Hat Virtualization Manager 4.4, including running the command **yum install rhvm**, but do not run **engine-setup**. See one of the *Installing Red Hat Virtualization* guides for more information.
6. Copy the backup file to the Red Hat Virtualization Manager 4.4 machine and restore it.

```
# engine-backup --mode=restore --file=backup.bck --provision-all-databases
```



NOTE

If the backup contained grants for extra database users, this command creates the extra users with random passwords. You must change these passwords manually if the extra users require access to the restored system. See <https://access.redhat.com/articles/2686731>.

7. Install optional extension packages if they were installed on the Red Hat Virtualization Manager 4.3 machine.

```
# yum install ovirt-engine-extension-aaa-ldap ovirt-engine-extension-aaa-misc ovirt-engine-extension-logger-log4j
```



NOTE

The configuration for these package extensions must be manually reapplied because they are not migrated as part of the backup and restore process.

- Decommission the Red Hat Virtualization Manager 4.3 machine if a different machine is used for Red Hat Virtualization Manager 4.4. Two different Managers must not manage the same hosts or storage.

The Red Hat Virtualization Manager 4.4 is now installed, with the cluster compatibility version set to 4.2 or 4.3, whichever was the preexisting cluster compatibility version.

Now you need to upgrade the remote databases in your environment.

Additional resources

- [Installing Red Hat Virtualization as a standalone Manager with local databases](#)
- [Installing Red Hat Virtualization as a standalone Manager with remote databases](#)

4.5. UPGRADING REMOTE DATABASES FROM POSTGRESQL 10 TO 12

Red Hat Virtualization 4.4 uses PostgreSQL 12, while RHV 4.3 uses PostgreSQL 10. If either of your databases (Manager or Data Warehouse) is installed on a separate machine, you must perform the following procedure on each remote database before upgrading the Manager.

TIP

This procedure uses the **pg_dump** and **pg_restore** commands. For a complete list of options for these commands, enter **pg_dump --help** or **pg_restore --help** on a machine with PostgreSQL installed.

- Back up all remote databases. Use the following command on each remote database machine:

```
# pg_dump -f backup-file database-name
```

The default name for the engine database is **engine**, and the default name for the Data Warehouse database is **ovirt-engine-history**.

For example, on the machine hosting the Data Warehouse database, enter a command similar to the following:

```
# pg_dump -f dwh-backup.dump ovirt-engine-history
```

- Copy the backup files to an external location such as a USB drive.

**NOTE**

This process requires installing Red Hat Enterprise Linux 8 on the Manager machine and all hosts, so make sure that you copy the backup file to a safe location.

3. Install Red Hat Enterprise Linux 8 on each database server, with the **Red Hat Virtualization** subscription attached.

For detailed installation instructions, see [Performing a standard RHEL installation](#).

The server must meet the minimum [Manager requirements](#).

4. Enable the correct repositories on each database server. For detailed instructions, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.4.

Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

5. Install the PostgreSQL server package:

```
# yum install postgresql postgresql-server postgresql-contrib
```

6. Restore the backup on the data warehouse database machine and the engine database machine:

```
# pg_restore -d database-name backup-file
```

7. On the Manager machine, run **engine-setup** to configure the Manager:

```
# engine-setup
```

You can now update the hosts.

4.6. MIGRATING HOSTS AND VIRTUAL MACHINES FROM RHV 4.3 TO 4.4

You can migrate hosts and virtual machines from Red Hat Virtualization 4.3 to 4.4 such that you minimize the downtime of virtual machines in your environment.

This process requires migrating all virtual machines from one host so as to make that host available to upgrade to RHV 4.4. After the upgrade, you can reattach the host to the Manager.

**WARNING**

When installing or reinstalling the host's operating system, Red Hat strongly recommends that you first detach any existing non-OS storage that is attached to the host to avoid accidental initialization of these disks, and with that, potential data loss.

Prerequisites

- Hosts for RHV 4.4 require Red Hat Enterprise Linux 8.2 or later. A clean installation of Red Hat Enterprise Linux 8.2 or later, or Red Hat Virtualization Host 4.4 is required, even if you are using the same physical machine that you use to run hosts for RHV 4.3.
- Red Hat Virtualization Manager 4.4 is installed and running.
- The compatibility level of the data center and cluster to which the hosts belong is set to 4.2 or 4.3. All data centers and clusters in the environment must have the cluster compatibility level set to version 4.2 or 4.3 before you start the procedure.

Procedure

1. Pick a host to upgrade and migrate that host's virtual machines to another host in the same cluster. You can use Live Migration to minimize virtual machine downtime. For more information, see [Migrating Virtual Machines Between Hosts](#) in the *Virtual Machine Management Guide*.
2. Put the host into maintenance mode and remove the host from the Manager. For more information, see [Removing a Host](#) in the *Administration Guide*.
3. Install Red Hat Enterprise Linux 8.2 or later, or RHVH 4.4. For more information, see [Installing Hosts for Red Hat Virtualization](#) in one of the *Installing Red Hat Virtualization* guides.
4. Install the appropriate packages to enable the host for RHV 4.4. For more information, see [Installing Hosts for Red Hat Virtualization](#) in one of the *Installing Red Hat Virtualization* guides.
5. Add this host to the Manager, assigning it to the same cluster. You can now migrate virtual machines onto this host. For more information, see [Adding Standard Hosts to the Manager](#) in one of the *Installing Red Hat Virtualization* guides.

Repeat these steps to migrate virtual machines and upgrade hosts for the rest of the hosts in the same cluster, one by one, until all are running Red Hat Virtualization 4.4.

Additional resources

- [Installing Red Hat Virtualization as a self-hosted engine using the Cockpit web interface](#)
- [Installing Red Hat Virtualization as a self-hosted engine using the command line](#)
- [Installing Red Hat Virtualization as a standalone Manager with local databases](#)
- [Installing Red Hat Virtualization as a standalone Manager with remote databases](#)

4.7. UPGRADING RHVH WHILE PRESERVING LOCAL STORAGE

Environments with local storage cannot migrate virtual machines to a host in another cluster because the local storage is not shared with other storage domains. To upgrade RHVH 4.3 hosts that have a local storage domain, reinstall the host while preserving the local storage, create a new local storage domain in the 4.4 environment, and import the previous local storage into the new domain.

Prerequisites

- Red Hat Virtualization Manager 4.4 is installed and running.

- The compatibility level of the data center and cluster to which the host belongs is set to 4.2 or 4.3.

Procedure

1. Ensure that the local storage on the RHVH 4.3 host's local storage is in maintenance mode before starting this process. Complete these steps:
 - a. Open the **Data Centers** tab.
 - b. Click the **Storage** tab in the **Details** pane and select the storage domain in the results list.
 - c. Click **Maintenance**.
2. Reinstall the Red Hat Virtualization Host, as described in [Installing Red Hat Virtualization Host](#) in the *Installation Guide*.



IMPORTANT

When selecting the device on which to install RHVH from the **Installation Destination** screen, do not select the device(s) storing the virtual machines. Only select the device where the operating system should be installed.

If you are using Kickstart to install the host, ensure that you preserve the devices containing the virtual machines by adding the following to the Kickstart file, replacing ``device`` with the relevant device.

```
# clearpart --all --drives=device
```

For more information on using Kickstart, see [Kickstart references](#) in *Red Hat Enterprise Linux 8 Performing an advanced RHEL installation*.

3. On the reinstalled host, create a directory, for example **/data** in which to recover the previous environment.

```
# mkdir /data
```

4. Mount the previous local storage in the new directory. In our example, **/dev/sdX1** is the local storage:

```
# mount /dev/sdX1 /data
```

5. Set the following permissions for the new directory.

```
# chown -R 36:36 /data
# chmod -R 0755 /data
```

6. Red Hat recommends that you also automatically mount the local storage via **/etc/fstab** in case the server requires a reboot:

```
# blkid | grep -i sdX1
/dev/sdX1: UUID="a81a6879-3764-48d0-8b21-2898c318ef7c" TYPE="ext4"
# vi /etc/fstab
UUID="a81a6879-3764-48d0-8b21-2898c318ef7c" /data ext4 defaults 0 0
```

7. In the Administration Portal, create a data center and select **Local** in the **Storage Type** drop-down menu.
8. Configure a cluster on the new data center. See [Creating a New Cluster](#) in the *Administration Guide* for more information.
9. Add the host to the Manager. See [Adding Standard Hosts to the Red Hat Virtualization Manager](#) in one of the *Installing Red Hat Virtualization* guides for more information.
10. On the host, create a new directory that will be used to create the initial local storage domain. For example:

```
# mkdir -p /localfs
# chown 36:36 /localfs
# chmod -R 0755 /localfs
```

11. In the Administration Portal, open the **Storage** tab and click **New Domain** to create a new local storage domain.
12. Set the name to **localfs** and set the path to **/localfs**.
13. Once the local storage is active, click **Import Domain** and set the domain's details. For example, define **Data** as the name, **Local on Host** as the storage type and **/data** as the path.
14. Click **OK** to confirm the message that appears informing you that storage domains are already attached to the data center.
15. Activate the new storage domain:
 - a. Open the **Data Centers** tab.
 - b. Click the **Storage** tab in the details pane and select the new data storage domain in the results list.
 - c. Click **Activate**.
16. Once the new storage domain is active, import the virtual machines and their disks:
 - a. In the **Storage** tab, select **data**.
 - b. Select the **VM Import** tab in the details pane, select the virtual machines and click **Import**. See [Importing Virtual Machines from a Data Domain](#) in the *Virtual Machine Management Guide* for more details.
17. Once you have ensured that all virtual machines have been successfully imported and are functioning properly, you can move **localfs** to maintenance mode.
18. Click the **Storage** tab and select **localfs** from the results list.
 - a. Click the **Data Center** tab in the details pane.
 - b. Click Maintenance, then click **OK** to move the storage domain to maintenance mode.
 - c. Click **Detach**. The Detach Storage confirmation window opens.
 - d. Click **OK**.

You have now upgraded the host to version 4.4, created a new local storage domain, and imported the 4.3 storage domain and its virtual machines.

You can now update the cluster compatibility version.

4.8. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.



IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.




IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

You can now update the cluster compatibility version for virtual machines in the cluster.

4.9. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

You can now update the data center compatibility version.

4.10. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

PART III. UPGRADING A SELF-HOSTED ENGINE ENVIRONMENT

CHAPTER 5. UPGRADING A SELF-HOSTED ENGINE FROM 4.2 TO RED HAT VIRTUALIZATION 4.3

Upgrading a self-hosted engine environment from version 4.2 to 4.3 involves the following steps:

1. [Make sure you meet the prerequisites, including enabling the correct repositories](#)
2. [Use the Log Collection Analysis tool to check for issues that might prevent a successful upgrade](#)
3. [Place the environment in global maintenance mode](#)
4. [Update the 4.2 Manager to the latest version of 4.2](#)
5. [Upgrade the Manager from 4.2 to 4.3](#)
6. [Disable global maintenance mode](#)
7. [Upgrade the self-hosted engine nodes, and any standard hosts](#)
8. [Update the compatibility version of the clusters](#)
9. [Reboot any running or suspended virtual machines to update their configuration](#)
10. [Update the compatibility version of the data centers](#)
11. If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, [you must replace the certificates now](#).

5.1. PREREQUISITES

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.4. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).

5.2. ANALYZING THE ENVIRONMENT

Run the Log Collection Analysis tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them.

The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

5.3. ENABLING GLOBAL MAINTENANCE MODE

You must place the self-hosted engine environment in global maintenance mode before performing any setup or upgrade tasks on the Manager virtual machine.

Procedure

1. Log in to one of the self-hosted engine nodes and enable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=global
```

2. Confirm that the environment is in global maintenance mode before proceeding:


```
# hosted-engine --vm-status
```

You should see a message indicating that the cluster is in global maintenance mode.

5.4. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.2. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt\*setup\* rh\*vm-setup-plugins
```

3. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.



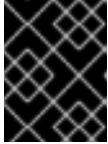
IMPORTANT

The update process might take some time. Do not stop the process before it completes.

4. Update the base operating system and any optional packages installed on the Manager:

■

```
# yum update
```

**IMPORTANT**

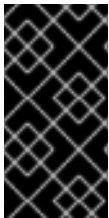
If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the update.

5.5. UPGRADING THE MANAGER FROM 4.2 TO 4.3

Upgrade the Red Hat Virtualization Manager from 4.2 to 4.3.

**IMPORTANT**

If the upgrade fails, the **engine-setup** command attempts to roll your Red Hat Virtualization Manager installation back to its previous state. For this reason, the previous version's repositories must not be removed until after the upgrade is complete. If the upgrade fails, detailed instructions display that explain how to restore your installation.

Procedure

1. Log in to the Manager virtual machine.
2. Enable the Red Hat Virtualization 4.3 repositories:

```
# subscription-manager repos \
  --enable=rhel-7-server-rhv-4.3-manager-rpms \
  --enable=jb-eap-7.2-for-rhel-7-server-rpms
```

All other repositories remain the same across Red Hat Virtualization releases.

3. Update the setup packages:

```
# yum update ovirt-*setup* rh-*vm-setup-plugins
```

4. Run **engine-setup** and follow the prompts to upgrade the Red Hat Virtualization Manager:

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

5. Disable the Red Hat Virtualization 4.2 repositories to ensure the system does not use any 4.2 packages:

```
# subscription-manager repos \
--disable=rhel-7-server-rhv-4.2-manager-rpms \
--disable=jb-eap-7-for-rhel-7-server-rpms
```

- Update the base operating system:

```
# yum update
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).



IMPORTANT

If any kernel packages were updated, reboot the machine to complete the upgrade.

5.6. DISABLING GLOBAL MAINTENANCE MODE

Procedure

- Log in to the Manager virtual machine and shut it down.
- Log in to one of the self-hosted engine nodes and disable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=none
```

When you exit global maintenance mode, `ovirt-ha-agent` starts the Manager virtual machine, and then the Manager automatically starts. It can take up to ten minutes for the Manager to start.

- Confirm that the environment is running:

```
# hosted-engine --vm-status
```

The listed information includes **Engine Status**. The value for **Engine status** should be:

```
{"health": "good", "vm": "up", "detail": "Up"}
```



NOTE

When the virtual machine is still booting and the Manager hasn't started yet, the **Engine status** is:

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

If this happens, wait a few minutes and try again.

You can now update the self-hosted engine nodes, and then any standard hosts. The procedure is the same for both host types.

5.7. UPDATING ALL HOSTS IN A CLUSTER

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See https://github.com/oVirt/ovirt-ansible-collection/blob/master/roles/cluster_upgrade/README.md for more information about the Ansible role used to automate the updates.

Update one cluster at a time.

Limitations


- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If the cluster has migration enabled, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.

Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster. The **Upgrade status** column shows if an upgrade is available for any hosts in the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.
 - **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.

- **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to `cluster_maintenance` during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.
5. Click **Next**.
 6. Review the summary of the hosts and virtual machines that will be affected.
 7. Click **Upgrade**.

You can track the progress of host updates:

- in the **Compute** → **Clusters** view, the **Upgrade Status** column shows **Upgrade in progress**
- in the **Compute** → **Hosts** view
- in the **Events** section of the **Notification Drawer** ().

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute** → **Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

5.8. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.



IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure


1. In the Administration Portal, click **Compute** → **Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

5.9. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

The Manager virtual machine does not need to be rebooted.

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute** → **Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

5.10. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute** → **Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

If you previously upgraded to 4.2 without replacing SHA-1 certificates with SHA-256 certificates, you must do so now.

5.11. REPLACING SHA-1 CERTIFICATES WITH SHA-256 CERTIFICATES

Red Hat Virtualization 4.4 uses SHA-256 signatures, which provide a more secure way to sign SSL certificates than SHA-1. Newly installed systems do not require any special steps to enable Red Hat Virtualization's public key infrastructure (PKI) to use SHA-256 signatures.

Preventing Warning Messages from Appearing in the Browser

1. Log in to the Manager machine as the root user.
2. Check whether `/etc/pki/ovirt-engine/openssl.conf` includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

3. Define the certificate that should be re-signed:

```
# names="apache"
```

4. Log in to one of the self-hosted engine nodes and enable global maintenance:

```
# hosted-engine --set-maintenance --mode=global
```

5. On the Manager, save a backup of the `/etc/ovirt-engine/engine.conf.d` and `/etc/pki/ovirt-engine` directories, and re-sign the certificates:

```
# ./etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
# for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
```

```
| sed \
    's;subject= \(.*\);1;' \
)"
/usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --san=DNS:"${ENGINE_FQDN}" \
    --keep-key
done
```

- Restart the **httpd** service:

```
# systemctl restart httpd
```

- Log in to one of the self-hosted engine nodes and disable global maintenance:

```
# hosted-engine --set-maintenance --mode=none
```

- Connect to the Administration Portal to confirm that the warning no longer appears.
- If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

Replacing All Signed Certificates with SHA-256

- Log in to the Manager machine as the root user.
- Check whether **/etc/pki/ovirt-engine/openssl.conf** includes the line **default_md = sha256**:

```
# cat /etc/pki/ovirt-engine/openssl.conf
```

If it still includes **default_md = sha1**, back up the existing configuration and change the default to **sha256**:

```
# cp -p /etc/pki/ovirt-engine/openssl.conf /etc/pki/ovirt-engine/openssl.conf."$(date
+ "%Y%m%d%H%M%S")"
# sed -i 's/^default_md = sha1/default_md = sha256/' /etc/pki/ovirt-engine/openssl.conf
```

- Re-sign the CA certificate by backing it up and creating a new certificate in **ca.pem.new**:

```
# cp -p /etc/pki/ovirt-engine/private/ca.pem /etc/pki/ovirt-engine/private/ca.pem."$(date
+ "%Y%m%d%H%M%S")"
# openssl x509 -signkey /etc/pki/ovirt-engine/private/ca.pem -in /etc/pki/ovirt-engine/ca.pem -
out /etc/pki/ovirt-engine/ca.pem.new -days 3650 -sha256
```

- Replace the existing certificate with the new certificate:

```
# mv /etc/pki/ovirt-engine/ca.pem.new /etc/pki/ovirt-engine/ca.pem
```


- Define the certificates that should be re-signed:

```
# names="engine apache websocket-proxy jboss imageio-proxy"
```

If you replaced the Red Hat Virtualization Manager SSL Certificate after the upgrade, run the following instead:

```
# names="engine websocket-proxy jboss imageio-proxy"
```

For more details see [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*.

- Log in to one of the self-hosted engine nodes and enable global maintenance:

```
# hosted-engine --set-maintenance --mode=global
```

- On the Manager, save a backup of the `/etc/ovirt-engine/engine.conf.d` and `/etc/pki/ovirt-engine` directories, and re-sign the certificates:

```
# ./etc/ovirt-engine/engine.conf.d/10-setup-protocols.conf
# for name in $names; do
  subject="$(
    openssl \
      x509 \
      -in /etc/pki/ovirt-engine/certs/"${name} ".cer \
      -noout \
      -subject \
    | sed \
      's;subject= \(.*\);!1;' \
  )"
  /usr/share/ovirt-engine/bin/pki-enroll-pkcs12.sh \
    --name="${name}" \
    --password=mypass \
    --subject="${subject}" \
    --san=DNS:"${ENGINE_FQDN}" \
    --keep-key
done
```

- Restart the following services:

```
# systemctl restart httpd
# systemctl restart ovirt-engine
# systemctl restart ovirt-websocket-proxy
# systemctl restart ovirt-imageio
```

- Log in to one of the self-hosted engine nodes and disable global maintenance:

```
# hosted-engine --set-maintenance --mode=none
```

- Connect to the Administration Portal to confirm that the warning no longer appears.
- If you previously imported a CA or https certificate into the browser, find the certificate(s), remove them from the browser, and reimport the new CA certificate. Install the certificate authority according to the instructions provided by your browser. To get the certificate

authority's certificate, navigate to **<http://your-manager-fqdn/ovirt-engine/services/pki-resource?resource=ca-certificate&format=X509-PEM-CA>**, replacing *your-manager-fqdn* with the fully qualified domain name (FQDN).

12. Enroll the certificates on the hosts. Repeat the following procedure for each host.
 - a. In the Administration Portal, click **Compute** → **Hosts**.
 - b. Select the host and click **Management** → **Maintenance** and **OK**.
 - c. Once the host is in maintenance mode, click **Installation** → **Enroll Certificate**.
 - d. Click **Management** → **Activate**.

CHAPTER 6. UPGRADING A SELF-HOSTED ENGINE FROM 4.3 TO RED HAT VIRTUALIZATION 4.4

Upgrading a self-hosted engine environment from version 4.3 to 4.4 involves the following steps:

1. [Make sure you meet the prerequisites, including enabling the correct repositories](#)
2. [Use the Log Collection Analysis tool to check for issues that might prevent a successful upgrade](#)
3. [Migrate any virtual machines that are running on the same host as the Manager virtual machine to another host in the same cluster.](#)
4. [Place the environment in global maintenance mode](#)
5. [Update the 4.3 Manager to the latest version of 4.3](#)
6. [Upgrade the Manager from 4.3 to 4.4](#)
7. [Upgrade the self-hosted engine nodes, and any standard hosts, while reducing virtual machine downtime.](#)
8. [\(Optional\) Upgrade RHVH while preserving local storage .](#)
9. [Update the compatibility version of the clusters](#)
10. [Reboot any running or suspended virtual machines to update their configuration](#)
11. [Update the compatibility version of the data centers](#)

6.1. PREREQUISITES

- Plan for any necessary virtual machine downtime. After you update the clusters' compatibility versions during the upgrade, a new hardware configuration is automatically applied to each virtual machine once it reboots. You must reboot any running or suspended virtual machines as soon as possible to apply the configuration changes.
- Ensure your environment meets the requirements for Red Hat Virtualization 4.4. For a complete list of prerequisites, see the [Planning and Prerequisites Guide](#).

6.2. ANALYZING THE ENVIRONMENT

Run the Log Collection Analysis tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them.

The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.3. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down
- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

6.3. MIGRATING VIRTUAL MACHINES FROM THE SELF-HOSTED ENGINE HOST

Only the Manager virtual machine should remain on the host until after you have finished upgrading the host. Migrate any virtual machines other than the Manager virtual machine to another host in the same cluster.

You can use Live Migration to minimize virtual machine down-time. For more information, see [Migrating Virtual Machines Between Hosts](#) in the *Virtual Machine Management Guide* for more information.

6.4. ENABLING GLOBAL MAINTENANCE MODE

You must place the self-hosted engine environment in global maintenance mode before performing any setup or upgrade tasks on the Manager virtual machine.

Procedure

1. Log in to one of the self-hosted engine nodes and enable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=global
```

2. Confirm that the environment is in global maintenance mode before proceeding:

```
# hosted-engine --vm-status
```

You should see a message indicating that the cluster is in global maintenance mode.

You can now update the Manager to the latest version of 4.3.

6.5. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.3. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt-*setup* rh*vm-setup-plugins
```

3. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

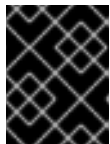
```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```

**NOTE**

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

**IMPORTANT**

The update process might take some time. Do not stop the process before it completes.

4. Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```

**IMPORTANT**

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the update.

You can now upgrade the Manager to 4.4.

6.6. UPGRADING THE RED HAT VIRTUALIZATION MANAGER FROM 4.3 TO 4.4

The Red Hat Virtualization Manager 4.4 is only supported on Red Hat Enterprise Linux 8.2 or later. You need to do a clean installation of Red Hat Enterprise Linux 8.2 or Red Hat Virtualization Host on the self-hosted engine host, even if you are using the same physical machine that you use to run the RHV 4.3 self-hosted engine.

The upgrade process requires restoring Red Hat Virtualization Manager 4.3 backup files onto the Red Hat Virtualization Manager 4.4 virtual machine.

Prerequisites

- All data centers and clusters in the environment must have the cluster compatibility level set to version 4.2 or 4.3 before you start the procedure.
- Make note of the MAC address of the self-hosted engine if you are using DHCP and want to use the same IP address. The deploy script prompts you for this information.

- During the deployment you need to provide a new storage domain for the Manager machine. The deployment script renames the 4.3 storage domain and retains its data to enable disaster recovery.

CAUTION

In an environment with multiple highly available self-hosted engine nodes, you need to detach the storage domain hosting the version 4.3 Manager after upgrading the Manager to 4.4. Use a dedicated storage domain for the 4.4 self-hosted engine deployment.

- If you use an external CA to sign HTTPS certificates, follow the steps in [Replacing the Red Hat Virtualization Manager CA Certificate](#) in the *Administration Guide*. The backup and restore include the 3rd-party certificate, so you should be able to log in to the Administration portal after the upgrade. Ensure the CA certificate is added to system-wide trust stores of all clients to ensure the foreign menu of virt-viewer works. See [BZ#1313379](#) for more information.



NOTE

Connected hosts and virtual machines can continue to work while the Manager is being upgraded.

Procedure

1. Log in to the Manager host machine.
2. Log in to the Manager virtual machine and shut down the engine service.

```
# systemctl stop ovirt-engine
```

3. Back up the Red Hat Virtualization Manager 4.3 environment.

```
# engine-backup --scope=all --mode=backup --file=backup.bck --log=backuplog.log
```

4. Copy the backup file to a storage device outside of the RHV environment.
5. Install RHVH 4.4 or Red Hat Enterprise Linux 8.2 or later on the node to use it as the self-hosted engine deployment host. See [Installing the Self-hosted Engine Deployment Host](#) for more information.
6. Install the self-hosted engine deployment tool.

```
# yum install ovirt-hosted-engine-setup
```

7. Copy the backup file to the host.
8. Log in to the Manager host and deploy the self-hosted engine with the backup file:

```
# hosted-engine --deploy --restore-from-file=/path/backup.bck
```

**NOTE**

tmux enables the deployment script to continue if the connection to the server is interrupted, so you can reconnect and attach to the deployment and continue. Otherwise, if the connection is interrupted during deployment, the deployment fails.

To run the deployment script using **tmux**, enter the **tmux** command before you run the deployment script:

```
# tmux
# hosted-engine --deploy --restore-from-file=backup.bck
```

The deployment script automatically disables global maintenance mode and calls the HA agent to start the self-hosted engine virtual machine. The upgraded host with the 4.4 self-hosted engine reports that HA mode is active, but the other hosts report that global maintenance mode is still enabled as they are still connected to the old self-hosted engine storage.

9. Detach the storage domain that hosts the Manager 4.3 machine. For details, see [Detaching a Storage Domain from a Data Center](#) in the *Administration Guide*.
10. Log in to the Manager virtual machine and shut down the engine service.

```
# systemctl stop ovirt-engine
```

11. Install optional extension packages if they were installed on the Red Hat Virtualization Manager 4.3 machine.

```
# yum install ovirt-engine-extension-aaa-ldap ovirt-engine-extension-aaa-misc ovirt-engine-extension-logger-log4j
```

**NOTE**

The configuration for these package extensions must be manually reapplied because they are not migrated as part of the backup and restore process.

The Red Hat Virtualization Manager 4.4 is now installed, with the cluster compatibility version set to 4.2 or 4.3, whichever was the preexisting cluster compatibility version.

Additional resources

- [Installing Red Hat Virtualization as a self-hosted engine using the Cockpit web interface](#)
- [Installing Red Hat Virtualization as a self-hosted engine using the command line](#)

You can now update the self-hosted engine nodes, and then any standard hosts. The procedure is the same for both host types.

6.7. MIGRATING HOSTS AND VIRTUAL MACHINES FROM RHV 4.3 TO 4.4

You can migrate hosts and virtual machines from Red Hat Virtualization 4.3 to 4.4 such that you minimize the downtime of virtual machines in your environment.

This process requires migrating all virtual machines from one host so as to make that host available to upgrade to RHV 4.4. After the upgrade, you can reattach the host to the Manager.



WARNING

When installing or reinstalling the host's operating system, Red Hat strongly recommends that you first detach any existing non-OS storage that is attached to the host to avoid accidental initialization of these disks, and with that, potential data loss.

Prerequisites

- Hosts for RHV 4.4 require Red Hat Enterprise Linux 8.2 or later. A clean installation of Red Hat Enterprise Linux 8.2 or later, or Red Hat Virtualization Host 4.4 is required, even if you are using the same physical machine that you use to run hosts for RHV 4.3.
- Red Hat Virtualization Manager 4.4 is installed and running.
- The compatibility level of the data center and cluster to which the hosts belong is set to 4.2 or 4.3. All data centers and clusters in the environment must have the cluster compatibility level set to version 4.2 or 4.3 before you start the procedure.

Procedure

1. Pick a host to upgrade and migrate that host's virtual machines to another host in the same cluster. You can use Live Migration to minimize virtual machine downtime. For more information, see [Migrating Virtual Machines Between Hosts](#) in the *Virtual Machine Management Guide*.
2. Put the host into maintenance mode and remove the host from the Manager. For more information, see [Removing a Host](#) in the *Administration Guide*.
3. Install Red Hat Enterprise Linux 8.2 or later, or RHVH 4.4. For more information, see [Installing Hosts for Red Hat Virtualization](#) in one of the *Installing Red Hat Virtualization* guides.
4. Install the appropriate packages to enable the host for RHV 4.4. For more information, see [Installing Hosts for Red Hat Virtualization](#) in one of the *Installing Red Hat Virtualization* guides.
5. Add this host to the Manager, assigning it to the same cluster. You can now migrate virtual machines onto this host. For more information, see [Adding Standard Hosts to the Manager](#) in one of the *Installing Red Hat Virtualization* guides.

Repeat these steps to migrate virtual machines and upgrade hosts for the rest of the hosts in the same cluster, one by one, until all are running Red Hat Virtualization 4.4.

Additional resources

- [Installing Red Hat Virtualization as a self-hosted engine using the Cockpit web interface](#)
- [Installing Red Hat Virtualization as a self-hosted engine using the command line](#)

- [Installing Red Hat Virtualization as a standalone Manager with local databases](#)
- [Installing Red Hat Virtualization as a standalone Manager with remote databases](#)

6.8. UPGRADING RHVH WHILE PRESERVING LOCAL STORAGE

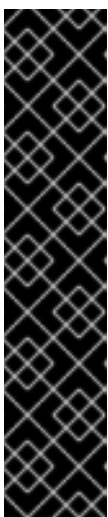
Environments with local storage cannot migrate virtual machines to a host in another cluster because the local storage is not shared with other storage domains. To upgrade RHVH 4.3 hosts that have a local storage domain, reinstall the host while preserving the local storage, create a new local storage domain in the 4.4 environment, and import the previous local storage into the new domain.

Prerequisites

- Red Hat Virtualization Manager 4.4 is installed and running.
- The compatibility level of the data center and cluster to which the host belongs is set to 4.2 or 4.3.

Procedure

1. Ensure that the local storage on the RHVH 4.3 host's local storage is in maintenance mode before starting this process. Complete these steps:
 - a. Open the **Data Centers** tab.
 - b. Click the **Storage** tab in the **Details** pane and select the storage domain in the results list.
 - c. Click **Maintenance**.
2. Reinstall the Red Hat Virtualization Host, as described in [Installing Red Hat Virtualization Host](#) in the *Installation Guide*.



IMPORTANT

When selecting the device on which to install RHVH from the **Installation Destination** screen, do not select the device(s) storing the virtual machines. Only select the device where the operating system should be installed.

If you are using Kickstart to install the host, ensure that you preserve the devices containing the virtual machines by adding the following to the Kickstart file, replacing ``device`` with the relevant device.

```
# clearpart --all --drives=device
```

For more information on using Kickstart, see [Kickstart references](#) in *Red Hat Enterprise Linux 8 Performing an advanced RHEL installation*.

3. On the reinstalled host, create a directory, for example **/data** in which to recover the previous environment.

```
# mkdir /data
```

4. Mount the previous local storage in the new directory. In our example, **/dev/sdX1** is the local storage:

```
# mount /dev/sdX1 /data
```

- Set the following permissions for the new directory.

```
# chown -R 36:36 /data
# chmod -R 0755 /data
```

- Red Hat recommends that you also automatically mount the local storage via **/etc/fstab** in case the server requires a reboot:

```
# blkid | grep -i sdX1
/dev/sdX1: UUID="a81a6879-3764-48d0-8b21-2898c318ef7c" TYPE="ext4"
# vi /etc/fstab
UUID="a81a6879-3764-48d0-8b21-2898c318ef7c" /data ext4 defaults 0 0
```

- In the Administration Portal, create a data center and select **Local** in the **Storage Type** dropdown menu.
- Configure a cluster on the new data center. See [Creating a New Cluster](#) in the *Administration Guide* for more information.
- Add the host to the Manager. See [Adding Standard Hosts to the Red Hat Virtualization Manager](#) in one of the *Installing Red Hat Virtualization* guides for more information.
- On the host, create a new directory that will be used to create the initial local storage domain. For example:

```
# mkdir -p /localfs
# chown 36:36 /localfs
# chmod -R 0755 /localfs
```

- In the Administration Portal, open the **Storage** tab and click **New Domain** to create a new local storage domain.
- Set the name to **localfs** and set the path to **/localfs**.
- Once the local storage is active, click **Import Domain** and set the domain's details. For example, define **Data** as the name, **Local on Host** as the storage type and **/data** as the path.
- Click **OK** to confirm the message that appears informing you that storage domains are already attached to the data center.
- Activate the new storage domain:
 - Open the **Data Centers** tab.
 - Click the **Storage** tab in the details pane and select the new data storage domain in the results list.
 - Click **Activate**.
- Once the new storage domain is active, import the virtual machines and their disks:
 - In the **Storage** tab, select **data**.

- b. Select the **VM Import** tab in the details pane, select the virtual machines and click **Import**. See [Importing Virtual Machines from a Data Domain](#) in the *Virtual Machine Management Guide* for more details.
17. Once you have ensured that all virtual machines have been successfully imported and are functioning properly, you can move **localfs** to maintenance mode.
18. Click the **Storage** tab and select **localfs** from the results list.
 - a. Click the **Data Center** tab in the details pane.
 - b. Click Maintenance, then click **OK** to move the storage domain to maintenance mode.
 - c. Click **Detach**. The Detach Storage confirmation window opens.
 - d. Click **OK**.

You have now upgraded the host to version 4.4, created a new local storage domain, and imported the 4.3 storage domain and its virtual machines.

6.9. CHANGING THE CLUSTER COMPATIBILITY VERSION

Red Hat Virtualization clusters have a compatibility version. The cluster compatibility version indicates the features of Red Hat Virtualization supported by all of the hosts in the cluster. The cluster compatibility is set according to the version of the least capable host operating system in the cluster.



IMPORTANT

To change the cluster compatibility version, you must have first updated all the hosts in your cluster to a level that supports your desired compatibility level. Check if there is an icon next to the host indicating an update is available.

Procedure


1. In the Administration Portal, click **Compute → Clusters**.
2. Select the cluster to change and click **Edit**.
3. On the **General** tab, change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Cluster Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.



IMPORTANT

An error message might warn that some virtual machines and templates are incorrectly configured. To fix this error, edit each virtual machine manually. The **Edit Virtual Machine** window provides additional validations and warnings that show what to correct. Sometimes the issue is automatically corrected and the virtual machine's configuration just needs to be saved again. After editing each virtual machine, you will be able to change the cluster compatibility version.

6.10. CHANGING VIRTUAL MACHINE CLUSTER COMPATIBILITY

After updating a cluster's compatibility version, you must update the cluster compatibility version of all running or suspended virtual machines by rebooting them from the Administration Portal, or using the REST API, instead of from within the guest operating system. Virtual machines that require a reboot are marked with the pending changes icon ().

The Manager virtual machine does not need to be rebooted.

Although you can wait to reboot the virtual machines at a convenient time, rebooting immediately is highly recommended so that the virtual machines use the latest configuration. Any virtual machine that has not been rebooted runs with the previous configuration, and subsequent configuration changes made to the virtual machine might overwrite its pending cluster compatibility changes.

Procedure

1. In the Administration Portal, click **Compute → Virtual Machines**.
2. Check which virtual machines require a reboot. In the **Vms:** search bar, enter the following query:

```
next_run_config_exists=True
```

The search results show all virtual machines with pending changes.

3. Select each virtual machine and click **Restart**. Alternatively, if necessary you can reboot a virtual machine from within the virtual machine itself.

When the virtual machine starts, the new compatibility version is automatically applied.



NOTE

You cannot change the cluster compatibility version of a virtual machine snapshot that is in preview. You must first commit or undo the preview.

6.11. CHANGING THE DATA CENTER COMPATIBILITY VERSION

Red Hat Virtualization data centers have a compatibility version. The compatibility version indicates the version of Red Hat Virtualization with which the data center is intended to be compatible. All clusters in the data center must support the desired compatibility level.



IMPORTANT

To change the data center compatibility version, you must have first updated the compatibility version of all clusters and virtual machines in the data center.

Procedure

1. In the Administration Portal, click **Compute → Data Centers**.
2. Select the data center to change and click **Edit**.
3. Change the **Compatibility Version** to the desired value.
4. Click **OK**. The **Change Data Center Compatibility Version** confirmation dialog opens.
5. Click **OK** to confirm.

PART IV. APPENDICES

APPENDIX A. UPDATES BETWEEN MINOR RELEASES

To update from your current version of 4.4 to the latest version of 4.4, update the Manager and then update the hosts.

A.1. ANALYZING THE ENVIRONMENT

Run the Log Collection Analysis tool prior to performing updates and for troubleshooting. The tool analyzes your environment for known issues that might prevent you from performing an update, and provides recommendations to resolve them.

The tool gathers detailed information about your system and presents it as an HTML file.

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.4. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. Install the Log Collection Analysis tool on the Manager machine:

```
# yum install rhv-log-collector-analyzer
```

2. Run the tool:

```
# rhv-log-collector-analyzer --live
```

A detailed report is displayed.

By default, the report is saved to a file called **analyzer_report.html**.

To save the file to a specific location, use the **--html** flag and specify the location:

```
# rhv-log-collector-analyzer --live --html=/directory/filename.html
```

3. You can use the ELinks text mode web browser to read the analyzer reports within the terminal. To install the ELinks browser:

```
# yum install -y elinks
```

4. Launch ELinks and open **analyzer_report.html**.

```
# elinks /home/user1/analyzer_report.html
```

To navigate the report, use the following commands in ELinks:

- **Insert** to scroll up
- **Delete** to scroll down

- **PageUp** to page up
- **PageDown** to page down
- **Left Bracket** to scroll left
- **Right Bracket** to scroll right

To update a standalone Manager, follow the standard procedure for minor updates:

A.2. UPDATING THE RED HAT VIRTUALIZATION MANAGER

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.4. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt-*setup* rh-*vm-setup-plugins
```

3. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.

**IMPORTANT**

The update process might take some time. Do not stop the process before it completes.

4. Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```

**IMPORTANT**

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#).

**IMPORTANT**

If any kernel packages were updated, reboot the machine to complete the update.

**NOTE**

If the update from RHV 4.2.7 to RHV 4.2.8 fails with a message indicating a dependency error with an **eap7-jboss-server-migration-wildfly** package:

1. Check if all the required repositories are enabled.
2. Update the **eap7-jboss-server-migration-wildfly** packages installed on the Manager:

```
# yum update eap7-jboss-server-migration-wildfly*
```

3. Run **engine-setup** again.

A.3. UPDATING A SELF-HOSTED ENGINE

To update a self-hosted engine from your current version to the latest version, you must place the environment in global maintenance mode and then follow the standard procedure for updating between minor versions.

Enabling global maintenance mode

You must place the self-hosted engine environment in global maintenance mode before performing any setup or upgrade tasks on the Manager virtual machine.

Procedure

1. Log in to one of the self-hosted engine nodes and enable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=global
```

2. Confirm that the environment is in global maintenance mode before proceeding:

```
# hosted-engine --vm-status
```

You should see a message indicating that the cluster is in global maintenance mode.

Updating the Red Hat Virtualization Manager

Prerequisites

- Ensure the Manager has the correct repositories enabled. For the list of required repositories, see [Enabling the Red Hat Virtualization Manager Repositories](#) for Red Hat Virtualization 4.4. Updates to the Red Hat Virtualization Manager are released through the Content Delivery Network.

Procedure

1. On the Manager machine, check if updated packages are available:

```
# engine-upgrade-check
```

2. Update the setup packages:

```
# yum update ovirt-*setup* rh*vm-setup-plugins
```

3. Update the Red Hat Virtualization Manager with the **engine-setup** script. The **engine-setup** script prompts you with some configuration questions, then stops the **ovirt-engine** service, downloads and installs the updated packages, backs up and updates the database, performs post-installation configuration, and starts the **ovirt-engine** service.

```
# engine-setup
```

When the script completes successfully, the following message appears:

```
Execution of setup completed successfully
```



NOTE

The **engine-setup** script is also used during the Red Hat Virtualization Manager installation process, and it stores the configuration values supplied. During an update, the stored values are displayed when previewing the configuration, and might not be up to date if **engine-config** was used to update configuration after installation. For example, if **engine-config** was used to update **SANWipeAfterDelete** to **true** after installation, **engine-setup** will output "Default SAN wipe after delete: False" in the configuration preview. However, the updated values will not be overwritten by **engine-setup**.



IMPORTANT

The update process might take some time. Do not stop the process before it completes.

4. Update the base operating system and any optional packages installed on the Manager:

```
# yum update
```



IMPORTANT

If you encounter a required Ansible package conflict during the update, see [Cannot perform yum update on my RHV manager \(ansible conflict\)](#) .



IMPORTANT

If any kernel packages were updated:

1. Disable global maintenance mode
2. Reboot the machine to complete the update.



NOTE

If the update from RHV 4.2.7 to RHV 4.2.8 fails with a message indicating a dependency error with an **eap7-jboss-server-migration-wildfly** package:

1. Check if all the required repositories are enabled.
2. Update the **eap7-jboss-server-migration-wildfly** packages installed on the Manager:

```
# yum update eap7-jboss-server-migration-wildfly*
```

3. Run **engine-setup** again.

Related Information

[Disabling global maintenance mode](#)

Disabling global maintenance mode

Procedure

1. Log in to the Manager virtual machine and shut it down.
2. Log in to one of the self-hosted engine nodes and disable global maintenance mode:

```
# hosted-engine --set-maintenance --mode=none
```

When you exit global maintenance mode, `ovirt-ha-agent` starts the Manager virtual machine, and then the Manager automatically starts. It can take up to ten minutes for the Manager to start.

3. Confirm that the environment is running:

```
# hosted-engine --vm-status
```

The listed information includes **Engine Status**. The value for **Engine status** should be:

```
{"health": "good", "vm": "up", "detail": "Up"}
```

**NOTE**

When the virtual machine is still booting and the Manager hasn't started yet, the **Engine status** is:

```
{"reason": "bad vm status", "health": "bad", "vm": "up", "detail": "Powering up"}
```

If this happens, wait a few minutes and try again.

A.4. UPDATING ALL HOSTS IN A CLUSTER

You can update all hosts in a cluster instead of updating hosts individually. This is particularly useful during upgrades to new versions of Red Hat Virtualization. See https://github.com/oVirt/ovirt-ansible-collection/blob/master/roles/cluster_upgrade/README.md for more information about the Ansible role used to automate the updates.

Update one cluster at a time.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If the cluster has migration enabled, virtual machines are automatically migrated to another host in the cluster.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines are shut down during the update, unless you choose to skip that host instead.


Procedure

1. In the Administration Portal, click **Compute** → **Clusters** and select the cluster. The **Upgrade status** column shows if an upgrade is available for any hosts in the cluster.
2. Click **Upgrade**.
3. Select the hosts to update, then click **Next**.
4. Configure the options:
 - **Stop Pinned VMs** shuts down any virtual machines that are pinned to hosts in the cluster, and is selected by default. You can clear this check box to skip updating those hosts so that the pinned virtual machines stay running, such as when a pinned virtual machine is running important services or processes and you do not want it to shut down at an unknown time during the update.
 - **Upgrade Timeout (Minutes)** sets the time to wait for an individual host to be updated before the cluster upgrade fails with a timeout. The default is **60**. You can increase it for

large clusters where 60 minutes might not be enough, or reduce it for small clusters where the hosts update quickly.

- **Check Upgrade** checks each host for available updates before running the upgrade process. It is not selected by default, but you can select it if you need to ensure that recent updates are included, such as when you have configured the Manager to check for host updates less frequently than the default.
 - **Reboot After Upgrade** reboots each host after it is updated, and is selected by default. You can clear this check box to speed up the process if you are sure that there are no pending updates that require a host reboot.
 - **Use Maintenance Policy** sets the cluster's scheduling policy to **cluster_maintenance** during the update. It is selected by default, so activity is limited and virtual machines cannot start unless they are highly available. You can clear this check box if you have a custom scheduling policy that you want to keep using during the update, but this could have unknown consequences. Ensure your custom policy is compatible with cluster upgrade activity before disabling this option.
5. Click **Next**.
 6. Review the summary of the hosts and virtual machines that will be affected.
 7. Click **Upgrade**.

You can track the progress of host updates:

- in the **Compute** → **Clusters** view, the **Upgrade Status** column shows **Upgrade in progress**
- in the **Compute** → **Hosts** view
- in the **Events** section of the **Notification Drawer** ().

You can track the progress of individual virtual machine migrations in the **Status** column of the **Compute** → **Virtual Machines** view. In large environments, you may need to filter the results to show a particular group of virtual machines.

You can also update hosts individually:

A.5. UPDATING INDIVIDUAL HOSTS

Use the host upgrade manager to update individual hosts directly from the Administration Portal.



NOTE

The upgrade manager only checks hosts with a status of **Up** or **Non-operational**, but not **Maintenance**.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If the cluster has migration enabled, virtual machines are automatically migrated to another host in the cluster. Update a host when its usage is relatively low.

- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines must be shut down before updating the host.

Procedure


1. Ensure that the correct repositories are enabled. To view a list of currently enabled repositories, run **dnf repolist**.

- For Red Hat Virtualization Hosts:

```
# subscription-manager repos --enable=rhvh-4-for-rhel-8-x86_64-rpms
```

- For Red Hat Enterprise Linux hosts:

```
# subscription-manager repos \
  --enable=rhel-8-for-x86_64-baseos-rpms \
  --enable=rhel-8-for-x86_64-appstream-rpms \
  --enable=rhv-4-mgmt-agent-for-rhel-8-x86_64-rpms \
  --enable=advanced-virt-for-rhel-8-x86_64-rpms \
  --enable=fast-datapath-for-rhel-8-x86_64-rpms
```

2. In the Administration Portal, click **Compute** → **Hosts** and select the host to be updated.
3. Click **Installation** → **Check for Upgrade** and click **OK**.
Open the **Notification Drawer** () and expand the **Events** section to see the result.
4. If an update is available, click **Installation** → **Upgrade**.
5. Click **OK** to update the host. Running virtual machines are migrated according to their migration policy. If migration is disabled for any virtual machines, you are prompted to shut them down. The details of the host are updated in **Compute** → **Hosts** and the status transitions through these stages:

Maintenance > **Installing** > **Reboot** > **Up**



NOTE

If the update fails, the host's status changes to **Install Failed**. From **Install Failed** you can click **Installation** → **Upgrade** again.

Repeat this procedure for each host in the Red Hat Virtualization environment.



NOTE

You should update the hosts from the Administration Portal. However, you can update the hosts using **dnf upgrade** instead.

A.6. MANUALLY UPDATING HOSTS

CAUTION

This information is provided for advanced system administrators who need to update hosts manually, but Red Hat does not support this method. The procedure described in this topic does not include important steps, including certificate renewal, assuming advanced knowledge of such information. Red Hat supports updating hosts using the Administration Portal. For details, see [Updating individual hosts](#) or [Updating all hosts in a cluster](#) in the *Administration Guide*.

You can use the **dnf** command to update your hosts. Update your systems regularly, to ensure timely application of security and bug fixes.

Limitations

- On RHVH, the update only preserves modified content in the **/etc** and **/var** directories. Modified data in other paths is overwritten during an update.
- If the cluster has migration enabled, virtual machines are automatically migrated to another host in the cluster. Update a host when its usage is relatively low.
- In a self-hosted engine environment, the Manager virtual machine can only migrate between self-hosted engine nodes in the same cluster. It cannot migrate to standard hosts.
- The cluster must have sufficient memory reserved for its hosts to perform maintenance. Otherwise, virtual machine migrations will hang and fail. You can reduce the memory usage of host updates by shutting down some or all virtual machines before updating hosts.
- Do not update all hosts at the same time, as one host must remain available to perform Storage Pool Manager (SPM) tasks.
- You cannot migrate a pinned virtual machine (such as a virtual machine using a vGPU) to another host. Pinned virtual machines must be shut down before updating the host.

Procedure

1. Ensure the correct repositories are enabled. You can check which repositories are currently enabled by running **dnf repolist**.

- For Red Hat Virtualization Hosts:

```
# subscription-manager repos --enable=rhvh-4-for-rhel-8-x86_64-rpms
```

- For Red Hat Enterprise Linux hosts:

```
# subscription-manager repos \
  --enable=rhel-8-for-x86_64-baseos-rpms \
  --enable=rhel-8-for-x86_64-appstream-rpms \
```

```
--enable=rhv-4-mgmt-agent-for-rhel-8-x86_64-rpms \
--enable=advanced-virt-for-rhel-8-x86_64-rpms \
--enable=fast-datapath-for-rhel-8-x86_64-rpms
```

2. In the Administration Portal, click **Compute** → **Hosts** and select the host to be updated.
3. Click **Management** → **Maintenance** and **OK**.
4. For Red Hat Enterprise Linux hosts:

- a. Identify the current version of Red Hat Enterprise Linux:

```
# cat /etc/redhat-release
```

- b. Check which version of the redhat-release package is available:

```
# dnf --refresh info --available redhat-release
```

This command shows any available updates. For example, when upgrading from Red Hat Enterprise Linux 8.2.z to 8.3, compare the version of the package with the currently installed version:

```
Available Packages
Name      : redhat-release
Version   : 8.3
Release   : 1.0.el8
...
```

CAUTION

The Red Hat Enterprise Linux Advanced Virtualization module is usually released later than the Red Hat Enterprise Linux y-stream. If no new Advanced Virtualization module is available yet, or if there is an error enabling it, stop here and cancel the upgrade. Otherwise you risk corrupting the host.

- c. If the Advanced Virtualization stream is available for Red Hat Enterprise Linux 8.3 or later, reset the **virt** module:

```
# dnf module reset virt
```



NOTE

If this module is already enabled in the Advanced Virtualization stream, this step is not necessary, but it has no negative impact.

You can see the value of the stream by entering:

```
# dnf module list virt
```

- d. Enable the **virt** module in the Advanced Virtualization stream with the **dnf module enable virt:8.y** command, where **y** is the version of the stream. For example, if the value for the stream is **8.3**, enter the following command:


```
# dnf module enable virt:8.3
```

5. Update the host:

```
# dnf upgrade --nobest
```

6. Reboot the host to ensure all updates are correctly applied.



NOTE

Check the `imgbased` logs to see if any additional package updates have failed for a Red Hat Virtualization Host. If some packages were not successfully reinstalled after the update, check that the packages are listed in `/var/imgbased/persisted-rpms`. Add any missing packages then run `rpm -Uvh /var/imgbased/persisted-rpms/*`.

Repeat this process for each host in the Red Hat Virtualization environment.

APPENDIX B. UPDATING THE LOCAL REPOSITORY FOR AN OFFLINE RED HAT VIRTUALIZATION MANAGER INSTALLATION

If your Red Hat Virtualization Manager is hosted on a machine that receives packages via FTP from a local repository, you must regularly synchronize the repository to download package updates from the Content Delivery Network, then update or upgrade that machine. Updated packages address security issues, fix bugs, and add enhancements.

1. On the system hosting the repository, synchronize the repository to download the most recent version of each available package:

```
# reposync --newest-only /var/ftp/pub/rhevrepo
```

This command might download a large number of packages, and take a long time to complete.

2. Ensure that the repository is available on the Manager machine, and then update or upgrade the machine.

B.1. ADDITIONAL RESOURCES

- See [Updating the Red Hat Virtualization Manager](#) for information on updating the Manager between minor versions.